XI

Exercice 1 (Loi(s) de réciprocité quadratique) Soit p un nombre premier impair. Soit z une racine primitive $p-$ième de l'unité.

a) Montrer que le groupe de Galois de $\mathbb{Q}(z)$ sur $\mathbb{Q}$ contient un seul sous-groupe d'indice 2.

b) En déduire que $s \in \mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ est un carré ssi $s \in \mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q})$ où $t := (-1)^{(p-1)/2}p$ (on rappelle que $\Delta = (-1)^{(p-1)/2}p^{p-2}$ est le discriminant du polynôme minimal de z sur $\mathbb{Q}$).

c) Soit q un nombre premier impair différent de p. On note $s_q \in \mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ l'élément qui envoie z sur z^q. Montrer que $s_q(t) = \left(\frac{q}{p}\right) t$.

d) Montrer que $s_q(t) = t^q \bmod q$ (dans $\mathbb{Z}[z]$).

e) En déduire la loi de réciprocité quadratique :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \ .$$

f) Soit y une racine primitive 8−ième de l'unité. Montrer que $(y+y^{-1})^2 = 2$. En déduire que :

$$(y + y^{-1})2^{(p-1)/2} = (y^p + y^{-p}) \bmod p$$

dans $\mathbb{Z}[y]$. Retrouver la loi de réciprocité complémentaire :

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p = \pm 1 \bmod 8, \\ -1 & \text{si } p = \pm 3 \bmod 8. \end{cases}$$

Exercice 2 (Discriminant d'un corps de nombres) Soit K un corps de nombres de degré n sur $\mathbb{Q}$. On note $s_1, ..., s_n$ les plongements de K dans $\mathbb{C}$. On suppose que $s_1, ..., s_{r_1}$ sont les plongements réels et que $s_{j+r_2} = \overline{s_j}$ si $r_1 + 1 \leq j \leq r_1 + r_2$.

On pose $s(x) := (s_1(x), ..., s_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$.

a) Soit A l'anneau des entiers de K. Montrer qu'il existe une base $x_1, ..., x_n$ de K sur $\mathbb{Q}$ formée d'éléments de A. Soit $y_1, ..., y_n$ la base duale relativement à la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}(xy)$. Montrer que $A \subseteq \mathbb{Z}y_1 \oplus ... \oplus \mathbb{Z}y_n$. En déduire que A est un $\mathbb{Z}-$ module libre de rang n.

b) Si $x_1, ..., x_n$ est une $\mathbb{Z}-$base de A, vérifier que le discriminant : $d := \det(\mathrm{Tr}(x_i x_j)_{1\leq i,j\leq n}) = \det(s_i(x_j))_{1\leq i,j\leq n}$ est indépendant de la base choisie. On dit que d est le *discriminant absolu de* K. Quel est le discriminant absolu de $\mathbb{Q}(z)$ si z est une racine primitive $p-$ème de l'unité, p premier ? Quel est le discriminant absolu de $\mathbb{Q}(\sqrt{d})$ où d est un entier sans facteur carré ?

c) Soit M un réseau de $\mathbb{R}^n$. On appelle *volume* de M le nombre :

$$v(M) := \mathrm{vol}\left(\{\sum_i t_i e_i \ : \ ^\forall i,\ 0 \leq t_i \leq 1\}\right)$$

pour n'importe quelle base $e_1, ..., e_n$ de M. Montrer que $v(s(A)) = 2^{-r_2}\sqrt{|d|}$ où d est le discriminant absolu de K.

d) Soit $0 \neq x \in A$. Montrer que $|N_{K/\mathbb{Q}}(x)| = |A/Ax|$. Si I est un idéal non nul de A, on notera $N(I) := |A/I|$ (c'est la *norme de* I). Montrer que $v(\sigma(I)) = 2^{-r_2}\sqrt{|d|}N(I)$.

e) Soit $t > 0$. On note :

$$B_t := \left\{ (y_1, ...y_{r_1}, z_1, ..., z_{r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ : \ \sum_i |y_i| + 2\sum_j |z_j| \leq t \right\} \ .$$

On admettra que $\mathrm{vol}(B_t) = 2^{r_1}(\pi/2)^{r_2} t^n/n!$.
Soit $0 \neq I$ un idéal de A.
On choisit t tel que $\mathrm{vol}(B_t) = 2^n v(s(I))$.
En déduire qu'il existe $x \in I$, non nul tel que

$$N_{K/\mathbb{Q}}(x) \leq (4/\pi)^{r_2} n!/n^n \sqrt{|d|} N(I) \ .$$

f) Montrer que $n = [K : \mathbb{Q}]$ est majoré indépendamment de K.

g) Soit B l'ensemble des $(y_1, ..., y_{r_2}, z_1, ..., z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tels que :

$$|y_1| \leq 2^n(\pi/2)^{-r_2}\sqrt{|d|}, \ |y_i| \leq 1/2, \ 2 \leq i \leq r_1,$$

$$|z_j| \leq 1/2, \ 1 \leq j \leq r_2$$

si $r_1 > 0$ et tels que

$$\Im(z_1) \leq 2^n(4/\pi)(\pi/2)^{-r_2}\sqrt{|d|}, \ \Re(z_1) \leq 1/4,$$

$$|z_j| \leq 1/2, \ 2 \leq j \leq r_2,$$

si $r_1 = 0$. Vérifier qu'il existe $0 \neq x \in K$ tel que $s(x) \in B$.Montrer que $K = \mathbb{Q}(x)$ et en déduire qu'il n'y a qu'un nombre fini de corps de nombres (dans $\mathbb{C}$) de discriminant d donné.

Exercice 3 (Théorème des unités) Soit K un corps de nombres de degré n sur $\mathbb{Q}$. On note $s_1, ..., s_n$ les plongements de K dans $\mathbb{C}$. On suppose que $s_1, ..., s_{r_1}$ sont les plongements réels et que $s_{j+r_2} = \overline{s_j}$ si $r_1 + 1 \leq j \leq r_1 + r_2$.
On pose $s(x) := (s_1(x), ..., s_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$.
On note A l'anneau des entiers de K et $A^\times$ son groupe des unités.

a) Montrer que si $x \in K$, alors :

$$x \in A^\times \Leftrightarrow N_{K/\mathbb{Q}}(x) = \pm 1 \ .$$

b) On pose $L : K^\times \to \mathbb{R}^{r_1+r_2}$, $x \mapsto (\log|s_1(x)|, ..., \log|s_{r_1+r_2}(x)|)$. Vérifier que c'est un morphisme de groupes.

c) Si B est une partie compacte de $\mathbb{R}^{r_1+r_2}$, montrer que $L^{-1}(B) \cap A^\times$ est fini. En déduire que $G := \ker L \cap A^\times$ est cyclique (fini). Montrer que G est le groupe des racines de l'unité de K.

d) Montrer que $L(A^\times)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2}$ (*i.e.* son intersection avec tout compact est finie). Montrer que $L(A^\times) \simeq G \times \mathbb{Z}^s$ pour un $s \leq r_1 + r_2 - 1$ *(indication :* $\prod_{1 \leq i \leq r_1} |s_i(x)| \prod_{r_1+1 \leq j \leq r_1+r_2} |s_j(x)|^2 = 1$*).*

e) Soit $a \geq 2^n(2\pi)^{-r_2}\sqrt{|d|}$. Soient $l := (l_1, ..., l_{r_1+r_2}) \in \mathbb{R}_{>0}^{r_1+r_2}$ tels que $\prod_{i=1}^{r_1} l_i \prod_{j=1}^{r_2} l_j^2 = a$. En considérant l'ensemble :

$$B := \left\{ (y_i, z_j) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ : \ |y_i| \leq l_i, \ |z_j| \leq l_j (^\forall \, i, j) \right\} ,$$

montrer qu'il existe $x_l \in A$ tel que

$$1 \leq |N(x_l)| \leq a$$

.
Vérifier que :

$$0 \leq \log l_i - log|s_i(x_l)| \leq \log a$$

pour tout i.

f) Soit $f : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ une forme linéaire non nulle sur l'hyperplan H d'équation $y_1 + ... + y_{r_1} + 2y_{r_1+1} + ... + 2y_{r_1+r_2} = 0$. Montrer qu'il existe $c_f > 0$ tel que :

$$|f(L(x_l)) - f(\log(l_1), ..., \log(l_{r_1+r_2}))| \leq c_f \log a \ .$$

Soit $b > c_f \log a$. Pour tout entier $h > 0$, il existe des réels $l_1, ...l_{r_1+r_2} > 0$ tels que :

$$\prod_{i=1}^{r_1} l_i \prod_{j=1}^{r_2} l_j^2 = a, \ f(\log(l_1), ..., \log(l_{r_1+r_2})) = 2bh$$

(le justifier !). On note $x_h \in A$ un élément tel que, comme ci-dessus :

$$|f(L(x_l)) - f(\log l)| \leq c_f \log a \ .$$

Vérifier que :

$$(2h-1)b < f(L(x_h)) < (2h+1)b$$

pour tout h. En déduire que les $L(x_h)$ sont deux a deux distincts, $h > 0$.

g) Vérifier que les idéaux Ax_h, $h > 0$, sont en nombre fini. En déduire l'existence d'un $u \in A^\times$ tel que $f(L(u)) \neq 0$.

h) Conclure que $L(A^\times)$ est de rang $r_1 + r_2 - 1$ et que :

$$A^\times \simeq G \times \mathbb{Z}^{r_1+r_2-1} \ .$$

i) *Application aux corps cyclotomiques :* Montrer que si p est un nombre prmeier impair, si z est une racine primitive $p-$ème de l'unité, alors on a un isomorphisme de groupes

$$\mathbb{Z}[z]^\times \simeq \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2} \ .$$

j) Quels sont les corps pour lesquels $A^\times$ est fini ?